North East Ambulance Service NHS
NHS Foundation Trust

Data Protection Policy

Document Control Sheet

Q Pulse Reference Number	POL-F-IMT-4
Version Number	V03
Document Author	Information Governance Manager
Lead Executive Director Sponsor	Director of Finance and Resources
Ratifying Committee	Finance Committee
Date Ratified	17 May 2018
Date Policy Effective From	17 May 2018
Next Review Date	16 May 2021
Keywords	Accountability; Article; biometrics; breach; Caldicott; commissioner; consent; contract; controller; DPA; GDPR; genetics; governance; health; identifiable; information; legal; legitimate; personal; principle; processing; processor; rights; SAR; schedule; sensitive; special; subject; vital.

Unless this copy has been taken directly from the Trust Quality Management site (Q-Pulse) there is no assurance that this is the most up to date version.

This policy supersedes all previous issues.

Version Control - Table of Revisions

All changes to the document must be recorded within the 'Table of Revisions'.

Version number	Document section/ page number	Description of change and reason (e.g. initial review by author/ requested at approval group	Author/ Reviewer	Date revised
01	All	First issue	IG Manager	Feb 2008
02	All	Revised in line with toolkit requirements. Renamed Data Protection Policy from Data Protection and Subject Access Policy. Subject Access Procedure and Form removed from appendix and contained in a separate document.	IG Manager	April 2009
02	All	Following ratification.	IG Manager	Sept 2009
2.1	Title	Policy title in Docuviewer changed to match document title and document owner added to profile box.	IG Manager	Nov 2009
2.2	Review date	Review date changed from 1 year to 2 years	IG Manager	Dec 2011
2.3	All	Following minor comments made by the Policy Review Group.	IG Manager	Mar 2012
3	E&D and Version control	E&D section moved Document control section moved to end	IG manager	May 2012
4	All	Minor organisation and policy reference updates	IG Manager	May 2014
2	All	Previous updates have never been uploaded to Q-Pulse so this policy will be version 2	Q-Pulse Admin	November 2016
2	All	Reformatting into new template	IG Manager	Sept 2016
3	All	Full review to take in account EU General Data Protection Regulation and UK Data Protection Bill.	IG Manager	May 2018

This page should not be longer than one single page.

Table of Contents

1. Introduction

This policy aims to detail how the Trust meets its legal obligations and NHS requirements concerning confidentiality and information security standards under the UK Data Protection Act (DPA) and the EU General Data Protection Regulation (GDPR).

The DPA seeks to empower individuals to take control of their personal data and to support organisations with their lawful processing of personal data. It supplements the GDPR as well as extends data protection laws to areas which are not covered by the GDPR. The DPA also ensures a single regime for the processing of personal data for law enforcement purposes across the whole of the law enforcement sector.

The DPA and GDPR legislates for the protection of personal information relating to living individuals. The Access to Health Records Act 1990 will remain relevant for information relating to deceased persons.

The nature of the work undertaken by the Trust's employees, volunteers and contractors brings them into possession of a great deal of confidential, and often highly sensitive information, both patient and staff related. Therefore, it is essential that the public at large have confidence that the organisation as a whole maintains confidentiality of information in whatever form it is given, to whoever it is given and for whatever purpose.

2. Purpose

The Trust is committed to a policy of protecting the rights and privacy of individuals (includes patients, staff and others) in accordance with the DPA. The Trust needs to process certain information about its staff, patients and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, monitor performance and to comply with legal obligations to funding bodies and government). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.

3. Scope

This policy covers both the Trust (North East Ambulance Service NHS Foundation Trust) and its subsidiary company North East Ambulance Service Unified Solutions (NEASUS). References to NEAS or Trust within this policy also cover NEASUS and its employees.

This policy covers all sites and systems operating and utilised by the Trust.

The policy applies to any individual employed, in any capacity, by the Trust, volunteer or contractor.

Other agencies and individuals working with the Trust, and who have access to

personal information, will be expected to have read and comply with this policy. It is expected that departments / sections who deal with external agencies will take responsibility for ensuring that such agencies sign a contract agreeing to abide by this policy.

4. Duties - Roles & Responsibilities

4.1 Trust Board

The Trust Board is collectively responsible for ensuring that the information risk management processes are providing them with adequate and appropriate information and assurances relating to risks against the Trust's objectives. The Trust as a body corporate is a data controller.

4.2 Chief Executive

The Chief Executive is ultimately responsible for the confidentiality and security of patient, staff and corporate information.

4.3 Director of Finance and Resources

The Director of Finance and Resources, who is also the Senior Information Risk Owner (SIRO) is the sponsor of this policy and has overall responsibility for the development and regular review of policies within their areas of responsibility.

4.4 Director of Quality and Safety (Executive Nurse)

Director of Quality and Safety (Executive Nurse) is also the Caldicott Guardian who has responsibility for:

- Reflecting patients' interests regarding the management and use of their records.
- Ensuring patient identifiable information is stored and shared in an appropriate and secure manner in line with the Caldicott Principles.

4.5 Information Governance Manager

The Information Governance Manager is also the Trust Data Protection Officer (DPO) and has responsibility for day-to-day data protection matters and for developing specific guidance notes on data protection issues. The DPO is responsible for ensuring payment of administrative fees in respect of DPA to the Information Commissioners Office (ICO). The DPO also has the responsibilities laid out in **Article 39 of the GDPR** – see Appendix A.

4.6 All staff

All staff within are responsible for ensuring that the principles outlined within this policy are universally applied. Compliance with DPA is the responsibility of all members of the Trust who process personal information and include contractors, temporary staff and students. Members of the Trust are responsible for ensuring that any personal data supplied to the Trust are accurate and up-to-date.

5. Glossary of Terms

This policy uses the following terms:

Term	Description
Data controller	The natural or legal person who alone or jointly with others determines the purpose and means of the processing of personal data.
Data processor	The natural or legal person which processes personal data on behalf of the controller.
Data subject	The identified or identifiable living individual to whom personal data relates.
Identifiable living individual	Living individual who can be identified, directly or indirectly, in particular by reference to: • An identifier such as a name, an identification number, location data or an online identifier; or • One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.
Information Commissioner	UK's independent body set up to uphold information rights.
Personal data	Information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing	In relation to personal data, means an operation or set of operations which is performed on personal data, or on sets of personal data, such as: • collection, recording, organisation, structuring or storage; • adaptation or alteration; • retrieval, consultation or use; • disclosure by transmission, dissemination or otherwise making available; • alignment or combination; or • restriction, erasure or destruction.

6. Policy Content

6.1 Data Protection Act

The DPA assists with and supplements the adoption of the GDPR into UK law. It strengthens or provides exceptions form some of the requirements of the GDPR and also extends data protection law into types of processing that are not covered by the GDPR. The DPA provides the Information Commissioner with additional functions and introduces new powers and offences in relation to data protection. The DPA applies to staff as well as patient records and covers both paper and electronic records.

Any individual has the right to see what information is held about them, and may challenge this information if they feel it is inaccurate or has caused damage to them. The DPA places obligations on those who record and use information about individuals. They must register the use of that information and they must ensure that they follow sound practices in recording and using the information.

6.2 Data protection principles

Article 5 of the GDPR requires that personal data shall be:

a) Processed lawfully, fairly and in a transparent manner in relation to individuals.

b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

6.3 Lawful basis for processing

There must be a valid lawful basis in order to process personal data. There are six available lawful bases for processing. No single basis is 'better' or more important than

the others – which basis is most appropriate to use will depend on the purpose and relationship with the individual.

The lawful basis must be determined and documented before processing. The Trust privacy notice should include the lawful basis for processing as well as the purposes of the processing. Processing of special category data requires both a lawful basis for general processing and an additional condition for processing.

The lawful bases for processing are set out in **Article 6 of the GDPR**. At least one of these must apply whenever you process personal data:

(a) **Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.

(b) **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).

(d) **Vital interests:** the processing is necessary to protect someone's life.

(e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

6.4 Special category data

When processing special category data, you need to identify both a lawful basis for processing (6.3) and a special category condition for processing in compliance with **Article 9 of the GDPR**. You should document both your lawful basis for processing and your special category condition so that you can demonstrate compliance and accountability.

Special category data is more sensitive, and so needs more protection. For example, information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. Your choice of lawful basis under **Article 6** does not dictate which special category condition you must apply, and vice versa. For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under **Article 9**. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example, if your lawful basis is vital interests, it is highly likely that the **Article 9** condition for vital interests will also be appropriate.

The conditions are listed in **Article 9(2) of the GDPR**:

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

(c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

(e) Processing relates to personal data which are manifestly made public by the data subject.

(f) Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

(g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

(h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.

(i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

(j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with **Article 89(1)** based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Section 10 and Schedule 1 of the DPA provide further clarification on assessment of whether there are lawful grounds to process special categories of personal data.

6.5 Individual rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

The lawful basis for your processing can also affect which rights are available to individuals. For example, some rights will not apply:

	Right to erasure	Right to portability	Right to object
Consent	✓	✓	×
Contract	✓	✓	×
Legal obligation	×	×	×
Vital interests	✓	×	×
Public task	×	×	✓
Legitimate interests	✓	×	✓

However, an individual always has the right to object to processing for the purposes of direct marketing, whatever lawful basis applies. The remaining rights are not always absolute, and there are other rights which may be affected in other ways. For example, your lawful basis may affect how provisions relating to automated decisions and profiling apply, and if you are relying on legitimate interests you need more detail in your privacy notice to comply with the right to be informed.

6.6 Data subject rights

Individuals have the right to access their personal data and supplementary

information. The right of access allows individuals to be aware of and verify the lawfulness of the processing. Further information is provided in the NEAS Subject Access Procedure.

6.7 Personal data breaches

All organisations must report certain types of personal data breach to the ICO within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, this must also inform those individuals without undue delay. Records of any personal data breaches must be kept, regardless of whether you are required to notify.

6.8 Accountability and governance

Accountability is one of the data protection principles - it makes the Trust responsible for complying with the GDPR and says that we must be able to demonstrate compliance. The Trust will:

- Put in place appropriate technical and organisational measures to meet the requirements of accountability.
- Adopt and implement data protection policies.
- Take a 'data protection by design and default' approach.
- Put written contracts in place with organisations that process personal data on our behalf.
- Maintain documentation of processing activities.
- Record and, where necessary, report personal data breaches.
- Carry out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests.
- Appoint a data protection officer.

The obligations that accountability places on the Trust are ongoing, it is not simply signing off a particular processing operation as 'accountable' and moving on. There must be a review of the measures implemented at appropriate intervals to ensure that they remain effective and updated where no longer fit for purpose.

Furthermore, if something does go wrong, then being able to show that the Trust actively considered the risks and put in place measures and safeguards can help provide mitigation against any potential enforcement action. On the other hand, if you good data protection practices cannot be shown, it may leave the Trust open to fines and reputational damage.

The administrative fine structure is shown in the table below:

€10m / 2% annual turnover	€20m / 4% annual turnover
Conditions applicable to child's consent in relation to information society services	Breach of data protection principles
Data protection by design and default	Data subject rights

Contract with processors	International transfers
Record of processing activities	
Appropriate security	
Breach notification	
Communication of breach to data subject	
DPIA DPO – position & tasks	

7. Training Required for Compliance with this Policy

All staff to receive mandatory data security training on an annual basis. Additional relevant training will also be undertaken by the SIRO, Caldicott Guardian and DPO.

8. Equality and Diversity

The Trust is committed to providing equality of opportunity. We aim to give people the freedom to flourish and develop in an environment free from discrimination, harassment, bullying and prejudice where their contributions, skills and knowledge are recognised and embraced.

We want to ensure that we provide services and employment opportunities that consider and are tailored to peoples' specific needs. Further details or our aims and objectives are outlined in our Equality Strategy – One Service for All.

We use the NHS England's Equality Delivery System 2 as our framework to monitor and improve our performance on equality and inclusion. We have also made a commitment to the Job Centre Two Ticks about Disability scheme, the Stonewall Work Place Equality Index meet our mandated requirements in relation to the Workforce Race Equality Standard and support a range of other initiatives.

This policy has been assessed to identify any potential for adverse or positive impact on specific groups of people protected by the Equality Act 2010 and does not discriminate either directly or indirectly.

The Trust values and respects the diversity of its employees and the communities it serves. In applying this policy we have considered eliminating unlawful discrimination, promoting equality of opportunity and, promoting good relations between people from diverse groups. Any issues highlighted in the assessment have been considered and incorporated into the policy and approved by the Head of Service/Director and relevant committee.

9. Monitoring Compliance with and Effectiveness of this Policy

9.1 Compliance and Effectiveness Monitoring

Arrangements for the monitoring of compliance with this policy and of the effectiveness of the policy are detailed below.

Monitoring Criterion	Response
Who will perform the monitoring?	Information Governance Manager
What are you monitoring?	Number of data protection incidents/breaches/complaints to ICO.
When will the monitoring be performed?	Every other month.
How are you going to monitor?	Via Ulysses reports.
What will happen if any shortfalls are identified?	Logged in risk registers.
Where will the results of the monitoring be reported?	Information Governance Working Group.
How will the resulting action plan be progressed and monitored?	The action plan will be progressed and monitored by the Information Governance Working Group.
How will learning take place?	Learning will be via the action plans and monitored by Information Governance Manager.

9.2 Compliance and Effectiveness Monitoring Table for this policy

Process in the policy	Monitoring and audit					
	Key Performance Indicators (KPI)/ Criteria	**Method**	**Who By**	**Committee**	**Frequency**	**Learning/ Action Plan**
Monitoring and reporting on Policy compliance	Number of data protection incidents	Via Safeguard reports	Information Governance Manager	IGWG	Bi-monthly	Add to risk registers
Report on subject access requests	No breaches	Report to IGWG	Information Governance Manager	IGWG	Bi-monthly	Add to risk registers

10. Consultation and Review of this Policy

This policy has been reviewed in consultation with the Information Governance Working Group, SIRO and Caldicott Guardian.

11. Implementation of this Policy

This Policy is to be implemented Trust wide through staff briefings, newsletters, team brief, divisional meetings

12. References

This document refers to the following guidance, including national and international standards:

- UK Data Protection Act (DPA)
- EU General Data Protection Regulation (GDPR)
- Access to Health Records Act 1990
- Caldicott Principles
- Information Commissioners Office
- Equality Act 2010

13. Associated Documentation

This policy refers to the following Trust documents:

- Subject Access Request Procedure

14. Appendices

14.1 Appendix A Article 39 GDPR – Tasks of the DPO

(1) The data protection officer shall have at least the following tasks:

a) To inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions.

b) To monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits.

c) To provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to **Article 35.**

d) To cooperate with the supervisory authority.

e) To act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in **Article 36**, and to consult, where appropriate, with regard to any other matter.

(2) The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.